Docket No.: S&ZIO020104

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

By: ______________________ Date: November 20, 2003

UNITED STATES IN THE PATENT AND TRADEMARK OFFICE

Applic. No.	:	10/662,627
Applicant	:	Astrid Elbe et al.
Filed	:	September 15, 2003
Art Unit	:	to be assigned
Examiner	:	to be assigned
Docket No.	:	S&ZIO020104
Customer No.	:	24131

LETTER

Hon. Commissioner for Patents

Sir:

Enclosed please find a copy of the English translation of the International Preliminary Examination Report for the above-identified application. Please enter it into the file.

Respectfully submitted,

____
For Applicants

LAURENCE A. GREENBERG
REG. NO. 29,308

Date: November 20, 2003

Lerner and Greenberg, P.A.
Post Office Box 2480
Hollywood, FL 33022-2480
Tel: (954) 925-1100
Fax: (954) 925-1101

/bmb

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference IO020104PCT	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/EP02/00734	International filing date (*day/month/year*) 24 January 2002 (24.01.02)	Priority date (*day/month/year*) 13 March 2001 (13.03.01)
International Patent Classification (IPC) or national classification and IPC G06F 7/72		
Applicant INFINEON TECHNOLOGIES AG		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   □ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of ______ sheets.

3. This report contains indications relating to the following items:

   I ☒ Basis of the report

   II □ Priority

   III □ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

   IV □ Lack of unity of invention

   V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

   VI □ Certain documents cited

   VII □ Certain defects in the international application

   VIII □ Certain observations on the international application

Date of submission of the demand 11 October 2002 (11.10.02)	Date of completion of this report 18 November 2002 (18.11.2002)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/EP02/00734

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

□ the international application as originally filed.

☒ the description, pages 1-24, as originally filed,
pages ______, filed with the demand,
pages ______, filed with the letter of ______,
pages ______, filed with the letter of ______.

☒ the claims, Nos. 1-13, as originally filed,
Nos. ______, as amended under Article 19,
Nos. ______, filed with the demand,
Nos. ______, filed with the letter of ______,
Nos. ______, filed with the letter of ______.

☒ the drawings, sheets/fig 1/7-7/7, as originally filed,
sheets/fig ______, filed with the demand,
sheets/fig ______, filed with the letter of ______,
sheets/fig ______, filed with the letter of ______.

2. The amendments have resulted in the cancellation of:

□ the description, pages ______
□ the claims, Nos. ______
□ the drawings, sheets/fig ______

3. □ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/EP 02/00734

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-13	YES
	Claims		NO
Inventive step (IS)	Claims	1-13	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-13	YES
	Claims		NO

2. Citations and explanations

1. The invention relates to a method for modular multiplication using a multiplication prediction method and a reduction prediction method as disclosed in document DE-A-3 631 992.

2. The disadvantage of this method is that, when calculating the ZDN algorithm, the additional ZDN register and the hardware comparator require extra chip area. However, the calculation of 2/3 N and the calculation of the auxiliary displacement value s_I in the ZDN algorithm, which is carried out by an iterative cycle, is time-critical for the whole algorithm and can quite possibly be decisive for the total withdrawal time of the algorithm.

3. The problem addressed by the present invention consists in producing an improved concept for modular multiplication which can be implemented in a space-saving manner and requires less computational time.

The present invention is based on the realisation that a computational time-intensive comparison of the updated intermediate result with the value ZDN, that is, two thirds of the module N, can be facilitated if the module N is first transformed into the transformed module N^T and the total modular multiplication is carried out with the transformed module N^T instead of the actual module.

As per the invention, the module is transformed such that the predetermined portion of the transformed module, that is, in a preferred embodiment, two thirds of the transformed module, becomes a specific number chosen such that it becomes trivial to compare 2/3 NT with the intermediate result Z. The transformation is carried out such that the predetermined portion of the transformed module has a higher order position with a first predetermined value that is followed by at least one lower order position which has a second predetermined value. The entire ZDN method is then carried out using N^T. A final inverse transformation which modularly reduces the transformation result of the modular multiplication using the original module N is required to produce the result CxM mod N.

5. The publication by Colin D. Walter: "Faster Modular Multiplication by Operand Scaling", Advances in Cryptology, Santa Barbara, 11-15 August 1991, pages 313-323 of the Proceedings of the Conference on Theory and Applications of Cryptographic Techniques (Crypto), Berlin, Springer, discloses a method for modular multiplication which uses operand scaling and in particular module scaling. The module M, which is based on on modular multiplication, is multiplied by a factor f such that the scaled module fM has a number of q highest value bits which are fixed. This makes it easier to calculate a function

quotient, since it is no longer dependent on the highest value bits of the scaled module, since the former are fixed. The function quotient is then carried out in a normal manner using the scaled module, whereupon up to 2f final subtractions from M take place from the output value of the function. Said document therefore discloses in general terms that a module can be scaled by multiplication with a number f so as to obtain a module having highest value bits which are fixed.